TESINA CISO (Chief Information Security Officer)

di Gianfrancoiunior De Carlo

Il continuo evolversi delle minacce informatiche e la crescita della complessità della sicurezza dovuta, sia alla maggiore "competenza" e abilità dei cyber criminali, sia all'ampliamento del perimetro di contenimento del rischio, rendono la governance della sicurezza un punto cruciale di ogni strategia aziendale.

Una volta si parlava di Responsabile della sicurezza o Security Manager, oggi, con le minacce legate allo sviluppo delle tecnologie digitali, le competenze legate alla gestione della sicurezza informatica si sono evolute, portando alla luce nuovi ruoli e nuove figure sempre più specializzate.

Oggi giorno i rischi di un cyber attacco sono sempre più elevati e, nel caso il pericolo si concretizzi, gli impatti per l'azienda possono essere tali da pregiudicarne l'operatività, intaccarne le risorse e creare danni difficili da risolvere. Meglio quindi prevenire, adottando le dovute misure di sicurezza.

Nasce così il CISO, all'anagrafe "Chief Information Security Office", un profilo professionale sempre più consolidato che, grazie a profonde competenze tecniche e relazionali, è in grado di assumere il ruolo di Responsabile della sicurezza informatica aziendale e non solo.

Con l'avvento della pandemia dovuta al Covid-19, molte aziende, di piccola e grande dimensione si sono trovate costrette ad utilizzare lo "smart working" che ha catapultato figure come il IT Manager, CIO e CISO in una nuova realtà. Nell'immediato questo cambiamento ha posto concretamente determinati rischi cyber che richiedono misure tecniche e organizzative adeguate unite a comportamenti corretti.

Una delle problematiche più rilevanti per gli smart worker è che lavorando da remoto possano utilizzare sia dotazioni aziendali sia, in molti casi, dispositivi di loro proprietà: spesso privi di patch di sicurezza e di protezione e, quindi, maggiormente esposti alle vulnerabilità, inoltre, i dati sensibili dell'organizzazione potrebbero muoversi al di fuori della rete aziendale così esponendoli al rischio di furti e hacking.

Ancora troppe aziende sottovalutano questi rischi, anche se l'avvicinarci dell'entrata in vigore del nuovo Regolamento europeo sulla protezione dei dati (Regolamento UE 2016/679) meglio noto come GDPR (General Data Protection Regulation) ha accesso un faro su questo tema. Le imprese stanno avviando processi per mettersi in regola e qualificare o introdurre figure manageriali in grado di gestire le problematiche di information security.

Gli analisti del ThreatTrack Security Report (VIPRE) già qualche tempo fa scrivevano che le aziende che impiegano un CISO sono significativamente più coscienti di quali siano le

minacce alla sicurezza, ma anche più fiduciose delle proprie capacità di difesa contro gli attacchi. Dotarsi di questo professionista è una decisione da non sottovalutare.
Considerando il contesto globale, infatti, la sicurezza informatica aziendale dev'essere trattata come una priorità.
Basti pensare che, come emerge dal report Clusit, nel triennio 2017-2019 il numero di cyber attacchi gravi analizzati è del +48%, passando da 1.127 a 1.670 annui.
Mentre uno studio realizzato dall'Osservatorio Information Security & Privacy del Politecnico di Milano sul finire del 2017 ha evidenziato come la figura del CISO sia formalizzata soltanto nel 46% delle aziende italiane, mentre nel 12% dei casi è di fatto presente anche se non è contemplata ufficialmente. Il più delle volte, poi, il CISO fa capo al CIO (Chief Information Officer).
Si tratta dunque di una scelta controproducente, visto che la priorità del CISO è invece principalmente la security, che può richiedere scelte in contrasto con altri criteri che il CIO potrebbe considerare prioritari, come la facilità di gestione o l'economicità di una soluzione IT.

Chi è il CISO?

Il CISO è il manager responsabile di definire una strategia di sicurezza informatica, di implementare programmi di protezione degli asset aziendali, di sviluppare e introdurre processi volti a mitigare i rischi informatici.
Il ruolo del CISO è proprio quello di conoscere le decisioni aziendali e progettare una strategia di sicurezza che permetta uno sviluppo del business il più possibile sicuro, inoltre deve anche tenere alta l'attenzione del management aziendale sugli aspetti di rischio legati a una cattiva gestione IT.

Sarà compito del Ciso, quindi, creare e fare in modo che si persegua, una strategia di sicurezza informatica aziendale efficace.

La confusione sul ruolo di questo esperto è data dalla presenza in azienda di professionisti come l'IT Manager. Banalmente, si potrebbe pensare che il coordinatore dell'area IT sia una figura adeguata e sufficiente per gestire l'ambito cyber security dell'organizzazione, ma non è così. L'IT manager ha enormi competenze tecniche in materia di informatica, ma per innalzare la sicurezza dell'intero perimetro aziendale e di conseguenza serve un approccio completo che spazi dalla conoscenza tecnologica allo sguardo sul business. Il Ciso sicuramente conosce la tecnologia, ma il suo è un ruolo specifico in ambito sicurezza per preservare le informazioni dell'azienda.

Il Ciso dovrebbe preoccuparsi di creare una cultura aziendale relativa alla cyber security, perché ancora oggi molte aziende non considerano il tema rilevante e urgente e di conseguenza non stanziano budget adeguati a questa area.

Il Ciso è un professionista dotato di digital skill che si ritrova in azienda a lavorare a stretto contatto con gli incaricati della compliance per garantire il rispetto dei vincoli

normativi. Importante, ad esempio, la collaborazione con il DPO (Data Protection Officer), figura nota perché espressamente citata nel GDPR ed obbligatoria in alcuni contesti come ad esempio nella Pubblica amministrazione.

Una premessa è d'obbligo, bisogna sottolineare che nei risultati dell'Osservatorio Information Security & Privacy 2020 che pur riportano un aumento degli investimenti in sicurezza (pari all'11% anno tra il 2018 e il 2019, per un valore assoluto di revenue riferito a quest'ultimo anno di 1,3 miliardi di euro) si riscontra ancora una scarsa maturità organizzativa e di gestione. In particolare, si legge che nel 40% delle imprese oggetto di osservazione la gestione dell'IT security è ancora affidata a CIO e IT ed è assente il CISO. Tale figura professionale è presente solo nel 27% delle organizzazioni interpellate.

Sembra infatti una questione di terminologie, invece ci sono differenze sostanziali rispetto ai compiti e all'impatto sull'organizzazione, il CISO ricopre una posizione quadro, come C-level.

Pertanto, un CISO ha un ruolo manageriale ed esecutivo di grado superiore. Il CISO si occupa di coordinare le iniziative di sicurezza rispetto ai programmi aziendali e agli obiettivi di business, assicurando che gli asset informativi e le tecnologie siano adeguatamente protetti.
Quando si parla di evoluzione del business, infatti, bisogna considerare le istanze portate dal BYOD – Bring your own device e dalla pervasività delle soluzioni mobile sempre più presenti in azienda, così come della virtualizzazione e del cloud o, ancora, i temi del big data management o ancora più a vasto raggio, il potenziamento e la relativa messa in sicurezza del data center.
Inevitabile per un CISO affinché il lavoro sia svolto in maniera ottimale è il confronto dello Shadow IT, un'espressione che si riferisce a servizi di information technology implementati e utilizzati all'interno di un'azienda senza l'approvazione dei responsabili dell'IT.

Una serie di azioni che escono dal controllo degli amministratori di rete e che non sono conformi con le disposizioni stabilite dall'azienda, rischiando di compromettere l'efficienza dei servizi e la qualità della business continuity aziendale, come ad esempio uso di applicazioni di messaggistica come WhatsApp o la sincronizzazione delle e-mail tra dispositivi mobili e desktop.
Il CISO è una figura che non dovrebbe occuparsi della parte più operativa quanto, piuttosto, di una risorsa di profilo consulenziale capace di impostare le linee guida delle policy di sicurezza e controllare che queste siano rispettate, di conseguenza necessita di un profilo ben delineato, con un forte carisma, leadership e problem solving.

Come opera il CISO?

In un momento storico in cui le imprese focalizzano il loro business in una sempre più massiccia presenza su Internet, quindi, il CISO deve avere un profilo operativo sempre più completo e deve essere in grado di affiancare alle proprie competenze tecniche, tecnologiche e organizzative, anche buone capacità relazionali e di coordinamento con gruppi di lavoro che possono essere complessi.

È fondamentale che il CISO abbia piena consapevolezza delle problematiche di cyber security all'interno dell'azienda per la quale lavora: solo così potrà comprendere quali sono i reali interessi economici e comunicare alla dirigenza i rischi derivanti dalle nuove minacce informatiche.

Questo discorso è ancor più vero se si considera che le tecnologie mobile, di virtualizzazione e di tipo cloud stanno diventando sempre più pervasive e presenti nelle aziende stesse, aumentando di fatto l'esposizione a minacce informatiche, introducendo nuove vulnerabilità.

Il CISO deve dunque dotarsi di competenze tecnologiche eterogenee e provvedere ad un aggiornamento tecnico costante proprio per essere in grado di fornire le soluzioni giuste e le contromisure necessarie da adottare per far fronte ad ogni nuova e sconosciuta tipologia di attacco. Oltre ad occuparsi della parte prettamente operativa di cyber security, il CISO deve avere anche un profilo consulenziale capace di impostare le linee guida delle policy di sicurezza e controllare che queste siano pienamente rispettate.

Il CISO, quindi, ha bisogno di guadagnare la fiducia e la stima di tutta l'azienda, il che può avvenire perseguendo tre obiettivi:

1. **L'importanza dell'informazione e della condivisione**. In primo luogo, il CISO deve lavorare sulla qualità della relazione e della comunicazione con il resto degli executive aziendali. È necessario un coinvolgimento a livello di vision ma anche di informazioni pragmatiche e concrete su rischi e possibili ripercussioni delle minacce sul business. Questo può essere fatto programmando l'elaborazione di un report mensile in cui vengono evidenziate gli incidenti, gli attacchi e i metodi di protezione sui canali più strategici: infrastrutture Web esterne, network, applicazioni legacy business critical e le esperienze di accesso interne, come le violazioni di accesso e le attività di account privilegiati. L'obiettivo è quello di informare ed educare gli executive in modo tale che, nell'eventualità che si verifichi un attacco, essi possano conoscere il protocollo di sicurezza adeguato, gestendo l'incidente con pragmatismo ed efficienza. In questo modo, il CISO evita che gli vengano attribuite colpe e responsabilità che non dipendono da lui, ma dai margini di rischio intrinsechi all'ICT.

2. **Il valore di una politica sempre aggiornata.** Il secondo obiettivo è quello di allineare le iniziative di sicurezza ai programmi aziendali e agli obiettivi di business, garantendo così che le risorse informative e le tecnologie siano adeguatamente protette. Questo implica il fatto che le iniziative di sicurezza devono essere basate su una gestione strategica del business, accettando un margine di rischio e considerando il TCO (Total Cost of Ownership) degli asset che vanno protetti. Inoltre, deve essere in grado di valutare quali misure di sicurezza e competenze debbano essere esternalizzate e quali no, facendo riferimento sempre al budget aziendale.

3. **La strategicità di un framework.** Il terzo obiettivo è utilizzare un framework consolidato per la sicurezza delle informazioni. Si tratta di un approccio fondamentalmente per progettare un sistema di protezione capace di ridurre rischi e vulnerabilità. In relazione al modello di business, alla compliance e all'instratruttura IT, il framework deve essere configurato ad hoc. Esistono diverse le opzioni tra cui scegliere: ISO 27001, COBIT e NIST 800-53 oppure il Framework nazionale per la sicurezza cybernetica, per esempio. Questo tipo di framework assicura che il programma per la sicurezza sia esaustivo e ben strutturato, includendo una compliance allineata all'azienda.

Appurata l'importanza del CISO all'interno dell'organizzazione aziendale, ci concentriamo ora su quelle che sono le competenze che vengono richieste.

Oltre alle ovvie competenze tecniche in merito alla sicurezza informatica acquisite sul campo, il CISO può ottenere anche una specifica certificazione come quella offerta da EC-Council (C-CISO) oppure il CISM (ISACA). Un'altra certificazione importante ma non necessaria è la CISA, prevalentemente incentrata sugli audit della sicurezza.

In particolare, il programma C|CISO (Certified CISO) si articola in cinque campi applicativi fornendo le relative competenze tecniche e applicative riassunte di seguito:

GOVERNANCE

- Definire, implementare, gestire e mantenere un programma di governance della sicurezza delle informazioni
- Creare una struttura di gestione della sicurezza dell'informazione
- Creare un quadro per il monitoraggio della governance della sicurezza dell'informazione tenendo conto delle analisi costi/benefici dei controlli e del ROI (Return on Investment)
- Comprendere gli standard, le procedure, le direttive, le politiche, i regolamenti e le questioni legali che riguardano il programma di sicurezza delle informazioni
- Conoscere i diversi standard come la serie ISO 27000

SECURITY RISK MANAGEMENT, CONTROLS, AUDIT MANAGEMENT

- Identificare i processi operativi e gli obiettivi aziendali per valutare il livello di tolleranza al rischio
- Progettare i controlli dei sistemi informativi in linea con le esigenze e gli obiettivi operativi e condurre test prima dell'implementazione per garantirne l'efficacia e l'efficienza
- Identificare e selezionare le risorse necessarie per implementare e mantenere efficacemente i controlli sui sistemi informativi
- Progettare e implementare controlli sui sistemi informativi per mitigare il rischio
- Progettare e condurre test sui controlli di sicurezza delle informazioni per garantire l'efficacia, individuare le carenze e garantire l'allineamento con le politiche, gli standard e le procedure dell'organizzazione
- Comprendere il processo di audit IT e avere familiarità con gli standard di audit IT
- Applicare i principi, le competenze e le tecniche di audit dei sistemi informativi per esaminare e testare le tecnologie e le applicazioni dei sistemi informativi al fine di progettare e attuare un'approfondita strategia di audit IT basata sul rischio
- Eseguire il processo di audit secondo gli standard stabiliti e interpretare i risultati in base a criteri definiti per assicurare che i sistemi informativi siano protetti, controllati ed efficaci nel supportare gli obiettivi dell'organizzazione
- Garantire che le necessarie modifiche basate sui risultati dell'audit siano attuate in modo efficace e tempestivo

SECURITY PROGRAM MANAGEMENT & OPERATIONS

- Definire le attività necessarie per eseguire con successo il progetto per la sicurezza delle informazioni
- Sviluppare, gestire e monitorare il budget di programma dei sistemi informativi, stimare e controllare i costi dei singoli progetti
- Identificare, negoziare, acquisire e gestire le risorse necessarie per una corretta progettazione e implementazione del programma sui sistemi informativi (ad esempio, persone, infrastrutture e architettura)
- Acquisire, sviluppare e gestire una squadra di progetto per la sicurezza delle informazioni
- Dirigere il personale addetto alla sicurezza delle informazioni e stabilire comunicazioni e attività di gruppo tra la squadra dei sistemi informativi e altro personale addetto alla sicurezza.

INFORMATION SECURITY CORE CONCEPTS

- Identificare i criteri per un controllo di accesso ai dati obbligatorio e discrezionale, comprendere i diversi fattori che aiutano nell'implementazione dei controlli di accesso e progettare un piano di controllo di accesso
- Identificare diversi sistemi di controllo dell'accesso, come carte d'identità e biometria

- Comprendere diversi concetti di ingegneria sociale e il loro ruolo negli attacchi che prendono di mira i dipendenti aziendali per sviluppare le migliori pratiche per contrastarli
- Elaborare un piano di intervento in caso di furto d'identità
- Identificare e progettare un piano per superare gli attacchi di phishing
- Identificare i processi di attenuazione e trattamento del rischio e comprendere il concetto di rischio accettabile
- Individuare le risorse necessarie per l'attuazione del piano di gestione dei rischi
- Progettare un processo sistematico e strutturato di valutazione dei rischi e stabilire, in coordinamento con gli stakeholder, un programma di gestione dei rischi per la sicurezza IT basato su standard e procedure
- Sviluppare, coordinare e gestire team di gestione del rischio
- Comprendere il rischio residuo nell'infrastruttura informativa
- Valutare le minacce e le vulnerabilità per identificare i rischi per la sicurezza e aggiornare regolarmente i controlli di sicurezza applicabili
- Sviluppare, implementare e monitorare piani di continuità operativa in caso di eventi dirompenti e garantire l'allineamento con gli obiettivi e gli scopi organizzativi
- Identificare le vulnerabilità e gli attacchi associati alle reti wireless e gestire i diversi strumenti di sicurezza per le reti wireless
- Valutare la minaccia di virus, trojan e malware per la sicurezza dell'organizzazione e identificare fonti e mezzi di infezione da malware

STRATEGIC PLANNING, FINANCE& VENDOR MANAGEMENT

- Eseguire analisi esterne dell'organizzazione (ad esempio, analisi di clienti, concorrenti, mercati e ambiente industriale) e interne (gestione dei rischi, capacità organizzative, misurazione delle prestazioni) e utilizzarle per allineare il programma di sicurezza delle informazioni con gli obiettivi dell'organizzazione
- Valutare e adeguare gli investimenti IT per garantire che siano sulla buona strada per supportare gli obiettivi strategici dell'organizzazione
- Acquisire e gestire le risorse necessarie per l'attuazione e la gestione del piano di sicurezza delle informazioni
- Monitorare e supervisionare la gestione dei costi dei progetti di sicurezza dell'informazione, il ritorno sugli investimenti (ROI) dei principali acquisti relativi alle infrastrutture IT e alla sicurezza e garantire l'allineamento con il piano strategico.

In generale, quindi, si capisce come sia opportuno che il CISO ricopra una posizione quadro all'interno dell'azienda, con un ruolo manageriale ed esecutivo. Il suo compito principale è quello di fare in modo che le iniziative di sicurezza siano coerenti con i programmi aziendali e gli obiettivi di business, garantendo che gli asset informativi e le tecnologie utilizzate vengano adeguatamente protetti.

Come diventare un CISO?

Il CISO deve naturalmente avere le competenze tecniche relative alla sicurezza informatica, a ciò si può aggiungere una certificazione specifica quale la C-CISO rilasciata dall'istituto statunitense EC-Council. Per esempio, i professionisti che otterranno tale certificazione potranno contare sulle competenze nei seguenti ambiti: Governance; IS Management Controls and Auditing Management; Management – Projects and Operations; Information Security Core Competencies; Strategic Planning & Finance.

Tutto ciò significa che le competenze del CISO devono spaziare dalla definizione e implementazione di un programma di governance e controllo della sicurezza delle informazioni per la propria azienda, all'identificazione dei processi operativi per sapere quale possa essere il livello di tolleranza al rischio, alla definizione delle attività da svolgere e a quali risorse assegnarle sino alla capacità di monitorare la spesa per i progetti di sicurezza e il relativo ROI- Return on investment.

Di seguito vi è un elenco delle principali caratteristiche di questa figura al centro della Cyber Security:

- **Leadership:** saper interagire con il consiglio di amministrazione in modo da influenzarne le decisioni, al fine di crescere a livello di posizionamento organizzativo grazie ad una leadership forte;
- **Pensiero strategico**: generare e implementare idee innovative e in linea con gli obiettivi aziendali;
- **Comunicazione**: saper comunicare le scelte per la gestione del rischio e spiegare le soluzioni tecnologiche adottate;
- **Team building**: capacità di costruire un team di specialisti in cyber security e di stabilire relazioni con gli executive e i decision maker principali dell'azienda;
- **Problem solving**: prendere decisioni in tempi rapidi, valutando le possibili conseguenze nel lungo termine;
- **Gestione delle crisi**: gestire le situazioni critiche e la relativa comunicazione;
- **Competenze tecnologiche**: conoscenza di minacce, vulnerabilità, rischi e sistemi per la protezione della sicurezza;
- **Comprensione del rischio**: capacità di comprendere i potenziali rischi, legata alla capacità previsionale di scenari futuri;
- **Approccio data-driven**: gestire, analizzare e utilizzare i dati a supporto delle decisioni;
- **Comprensione delle regolamentazioni**: per raccogliere e trattare i dati online occorre conoscere le regolamentazioni in vigore nei diversi Paesi e le relative implicazioni in materia di sicurezza e protezione dei dati.

Comprendendo quali sono le azioni che il Ciso deve intraprendere, è chiaro quindi che si tratta di un professionista con non solo competenze tecniche, ma anche manageriali. Deve essere assolutamente in grado di individuare le corrette risorse interne e i fornitori giusti per portare avanti la strategia di sicurezza informatica aziendale. Ha una cultura economico-finanziaria di base importante, poiché le ripercussioni degli incidenti

informatici sono economiche, tanto che per le aziende quotate in Borsa possono comportare un oscillamento del titolo. Il Ciso deve sapere come funziona il bilancio e il mercato, deve conoscere la differenza tra un investimento e un costo per consigliare al meglio l'azienda. Deve avere, quindi, insomma un approccio risk based, che consiste anche nel riuscire a capire quanto allocare in budget all'organizzazione e in che periodo e ambito, cercando di sfruttare ad esempio eventuali finanziamenti nazionali.

Sono sicuramente da non trascurare anche le competenze normative. Il Ciso deve conoscere gli articoli del GDPR che lo riguardano e avere un linguaggio condiviso con l'ufficio legale aziendale per collaborare in maniera proficua. È importante che abbia anche un'infarinatura da giuslavorista, perché alcuni strumenti da adottare per la security rischiano di violare lo statuto dei lavoratori. Oltre a ciò, il Ciso dovrà essere dotato di capacità comunicative e comprendere come ragionano le persone. Infatti, uno dei principali vettori di rischio informatico è il fattore umano e il CISO, dunque, si dovrà preoccupare di predisporre adeguata formazione al personale.

All'interno dell'azienda, la prima mansione che spetteranno al CISO è quella di effettuare gli ASSESSMENT INIZIALI:

-Creare un action plan e una strategia di lungo termine
- Implementare le necessarie policy
-Gestire gli aspetti di compliance (ad esempio il GDPR)
-Gestire la classificazione delle informazioni
-Gestire l'asset management
- Gestire i diritti di accesso alle risorse e informazioni
- Gestire le protezioni perimetrali nonché le reti wi-fi
- Prevenire gli attacchi ed indirizzare attività di hardening, Patch e vulnerability management
- Gestire le identità digitali
- Gestire gli incidenti
- Gestire la formazione del personale
- Riportare in modo diretto ai vertici aziendali

Per quanto riguarda la gestione degli incidenti, oggi giorno le minacce più costanti per avvengono ai fornitori; infatti, un attacco informatico a un fornitore potrebbe comportare non solo la perdita di dati sensibili, ma anche di strategia aziendale o segreti commerciali, causando un'interruzione operativa così lunga da compromettere la capacità dell'azienda di produrre beni o servizi.
Di conseguenza è bene dotarsi di Supply Chain Security per proteggere il fornitore ma soprattutto la propria azienda.

CISO interno O CISO outsourcing ?

Sebbene la professionalità del CISO sia indispensabile per assicurare la sicurezza delle medie e grandi imprese, gestire una figura di questo genere in house può risultare estremamente oneroso, talvolta con costi e attività non sempre in linea con le esigenze aziendali.

La soluzione arriva dalla **gestione in outsourcing** del servizio, appoggiandosi ad aziende partner in grado di fornire supporto multidisciplinare in maniera "sartoriale", personalizzata secondo le necessità dell'impresa. In questo modo si risparmiano costi e tempo, oltre a migliorare la propria brand awareness posizionandosi come una realtà attenta alla sicurezza dei propri sistemi, alla data protection e rispettosa delle regole.

Tuttavia, assumere nella propria impresa un CISO professionista come dipendente è un'operazione costosa. Non solo, ma anche impegnativa dal punto di vista dei costi nel tempo, in quanto bisognerà dedicare budget alla figura in sé e non a un progetto orientato a soddisfare altre necessità aziendali.
Ingaggiare invece un CISO esterno consente di superare questi problemi e trarre il massimo beneficio dalla attività di questa figura. In pratica si tratta di affidare il servizio in outsourcing, non assumendo direttamente il professionista nell'organigramma aziendale ma appoggiandosi a un'azienda di advisory che fornisce tutte le competenze e l'assistenza necessarie all'espletamento di adempimenti e controlli mirati.

I vantaggi dell'outsourcing permettono di disporre di un professionista sempre aggiornato senza che l'azienda debba farsi carico dei costi di formazione. Un professionista esterno, alla luce della sua esperienza in molteplici realtà, potrà infatti consigliare al meglio l'azienda ed esercitare un importante ruolo terzo, del tutto estraneo alle eventuali logiche di potere interne. Soprattutto per questo motivo, la scelta di un CISO esterno è certamente una scelta estremamente delicata, ma la sua indipendenza e la sua capacità di essere *super partes* in una logica consulenziale potrà aiutare l'azienda nella scelta delle soluzioni più adatte, a differenza di quanto potrebbe fare un system integrator, interessato a spingere prodotti suoi o dei partner.
Inoltre, data la sua esperienza ha una maggior consuetudine alle relazioni con **i** vertici aziendali ed è dunque più adatto ad interfacciarsi con il top management.

Un CISO deve essere in grado, infatti, di operare in situazioni complesse, come quelle che si determinano in caso di incidente, quando potrebbe trovarsi nella situazione di coordinare un team tecnico che sta lavorando per ripristinare l'operatività, un team legale che sta operando per sporgere la denuncia presso le autorità competenti, un team focalizzato sulla protezione dei dati personali, che deve notificare la violazione al Garante,un team per la comunicazione che deve adoperarsi per prevenire danni all'immagine aziendale. Solo chi ha sperimentato in più occasioni situazioni di questo tipo e ha un approccio multidisciplinare riesce a non perdere la testa ed essere davvero efficace.

In sintesi, è preferibile scegliere come outsourcer un'azienda che non si limiti a mettere disposizione un CISO esperto ma offra anche il supporto di un team con competenze multidisciplinari integrate, organizzative, legali, tecnologiche e di security, per poter svolgere al meglio il ruolo di CISO in qualunque circostanza.

SITIOGRAFIA

- Osservatori.net, Giorgia Dragoni (https://blog.osservatori.net/it_it/ciso-cosa-fa-responsabile-security)

- Network digital 360, Redazione (https://www.zerounoweb.it/techtarget/searchsecurity/cybersecurity/quanto-e-importante-la-figura-del-ciso-in-azienda/)

- Advisory 360 Hub (https://www.p4ihub.it/blog/cybersecurity/ciso-as-a-service/sicurezza-informatica-aziendale-il-ruolo-del-ciso/)
https://www.advisory360hub.it/blog/cybersecurity/ciso-as-a-service/ciso-i-vantaggi-di-scegliere-loutsourcing/

- Cybersecurity360 (https://www.cybersecurity360.it/cultura-cyber/ciso-che-fa-e-come-si-diventa-chief-information-security-officer/)

- Rapporto Clusit 2021 (ottobre-marzo)